(12) UK Patent Application (19) GB (11) 2 358 115 (13) A

(43) Date of A Publication 11.07.2001

(21) Application No 0022614.2

(22) Date of Filing 15.09.2000

(30) Priority Data
(31) 09398028 (32) 17.09.1999 (33) US

(51) INT CL[7]
H04L 9/30 // G06F 1/00 , H04N 1/44

(52) UK CL (Edition S)
H4P PDCSC

(56) Documents Cited
GB 2336512 A EP 0935182 A1 WO 96/25812 A1

(58) Field of Search
UK CL (Edition S) H4P PDCSA PDCSC PDCSX
INT CL[7] G06F 1/00 , G06K 19/06 , G07D 7/00 , H04L 9/00 9/30 9/32 , H04N 1/32 1/44
Online Databases: WPI, EPODOC, JAPIO

(71) Applicant(s)
International Business Machines Corporation
(Incorporated in USA - New York)
Armonk, New York 10504, United States of America

(72) Inventor(s)
Gordon Wesley Braudaway
Patrick D Howard
Pasumarti Venkata Kamesam
Frederick Cole Mintzer
Howard Edward Sachar
Sean William Smith
John Mark Socolofsky
Charles Philippe Louis Tresser
Chai Wah Wu

(74) Agent and/or Address for Service
G M Zerbi
IBM United Kingdom Limited, Intellectual Property Dept, Hursley Park, WINCHESTER, Hampshire, SO21 2JN, United Kingdom

(54) Abstract Title
Method and system for remote printing of duplication resistant documents

(57) A communication link is provided between a certified document owner and a remote printing station. The printing station is provided with a leaf of special paper and determines whether the leaf is legitimate by comparing a representative number and its encrypted version (encrypted using a first key) at locations on the leaf Extra hidden data may also be provided on the leaf for checking its authenticity. The printing station transmits the representative number and its encrypted version to the certified document owner who can also perform the authenticity check. The certified document owner appends a document with the representative number, computes a digitally signed version of the appended document (using a second key) and transmits the document and the signed version to the printing station for printing. As such, further unauthorised prints of this document as well as copies of this document can be recognized as non-authentic. The printer used does not need to be specialised with security controls.

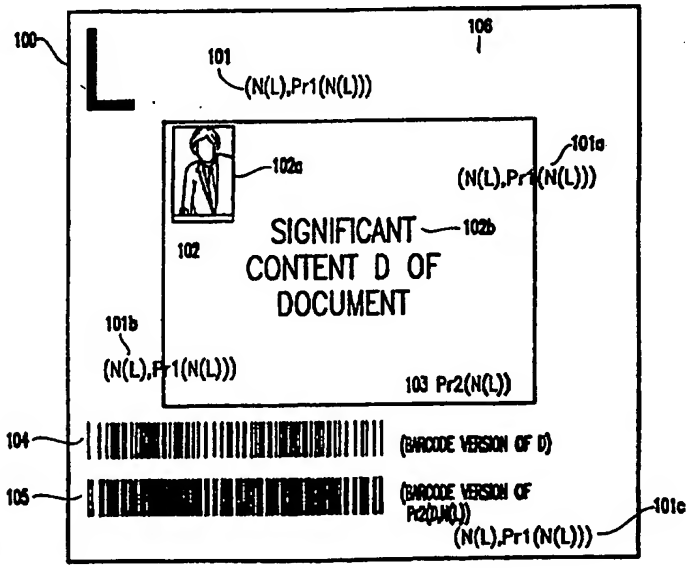

FIG.1A

GB 2 358 115 A

METHOD AND SYSTEM FOR REMOTE PRINTING OF DUPLICATION-RESISTANT DOCUMENTS

Field of the Invention

The present invention generally relates to the field of digitized imaging and document security, and is more specifically directed to a system and method which allows remotely printing a document using printers belonging to third parties and generally not equipped with special secure control units, such that additional prints and copies of the same document are recognizable as non-authentic using publicly available means.

Description of the Related Art

Presently, there is a problem of remotely printing a document using printers belonging to third parties and generally not equipped with special secure control units, such that additional prints and copies of the same document are difficult, if not impossible, to recognize as non-authentic.

There are many different situations in which such a problem surfaces, but which the conventional systems and methods cannot remedy. Hereinbelow are described some exemplary situations, and it will be evident to one of ordinary skill in the art that there are many more such situations in which such a capability would be useful.

For example, such a capability would be useful for "certified documents". Such documents refer to a class of documents that has no intrinsic value, such as bearer bonds, but has content that is authenticated and vouched for by an appropriate authority. "Certified documents" would include vital records (i.e., birth certificates, death certificates, marriage certificates, etc.), professional licenses, official surveys, inspection reports, university transcripts, legal briefs, etc.

Another area in which such a capability would be useful is "*titles*" and documents relating thereto. That is, "titles" are documents which have a value of their own, at least for some span of time, and are therefore negotiable. Some examples would include ownership certificates and some type of insurance contracts, such as "Certificates of Insurance", which are issued by insurance companies as proof that a consignment or a package of goods is indeed insured. Corporations that ship/transport goods regularly require a facility whereby certificates of insurance can be issued quickly, and require that such a certificate be printed remotely. It is further necessary to ensure that such certificates cannot be duplicated (copied).

Yet another example is "Financial instruments" and other documents of value, such as money orders, certified checks, gift certificates, and tickets (e.g., for transportation, entertainment, sporting events, etc.).

In all the above cases, care must be taken to prevent copies and additional prints from being produced to look like and to be used as authentic documents. This need is obvious in the "title" and "financial instrument" cases, as they are negotiable objects, and in some other examples mentioned above.

For certified documents, there is a compelling need in electronic commerce for processes to maintain "electronic originals". In the physical world (e.g., the so-called "real world"), original documents are typically authenticated through visual inspection of "raised seals" (e.g., notary seals or the like by persons specially commissioned for such tasks as notarization and the like), embossed signatures, and special bond paper. Social and commercial processes are dependent on the ability of two parties to authenticate documents as originals and to detect any tampering thereof.

Because of the proliferation of computers attached to networks (e.g., which all together cover the entire planet), it has been proposed to replace such documents by electronic documents. Using modern cryptographic techniques, electronic documents can indeed be created which contain: a) a proof of authenticity; and b) a non-counterfeitable list of successive legitimate owners.

The property a) is what is needed for a certificate, while a) and b) together are required for an electronic title, so that paper versions seem unnecessary in the new electronic era. It is noted that in particular that electronic money transactions have been used for several years already.

However, the ease of creating electronic certificates and titles does not completely alleviate the need for paper versions.

First of all, access to data networks is not yet as pervasive as it can be, and will not be in the foreseeable future. Secondly, a combination of legal and psychological factors likely will not make paper documents obsolete in the near future. For example, the number of pages printed on paper is still growing in the countries most linked to the Internet.

Thus, providing a mechanism and capability to print remotely with the possibility to identify illegal copies thus would be quite valuable, and such a capability would allow usage of some benefits of the network of computers. Hitherto the invention, such a capability has not existed.

Further, it is noted that mechanisms for identifying photocopies as such have been known and used for many years. For example, such a mechanism is disclosed in US Patent No. 4,341,404, issued to Mowry, Jr., et al., incorporated herein by reference. In most cases, photocopy protection is insured by printing some fine structure on the background of the document. These fine structures either are absent from the copy, or some text such as "COPY" or "VOID" appears on the copy, or a combination of change of background and visible disqualifying word is used. In the case that the printer used to complete the print of the document can print as finely as needed, the photocopy-protecting background can be printed at the same time as the rest of the document. Otherwise, the protecting background can be printed before the significant part of the document. Paper carrying a photocopy-protecting background will be called *photocopy-protected paper* hereinbelow.

It is assumed that such photocopy-protected paper is used for remote printing, and it is noted that an easy, although quite superficial, test of authenticity of the documents is provided by simply checking that a photocopy of the document caries the mark which characterizes the chosen photocopy evidence mechanism. Such photocopy protected paper is available from a number of sources including Verify First Technologies of Paso Robles, CA. Additionally, it is noted that US Patent No. 5,377,271, issued to Foreman et al. and incorporated herein by reference, addresses the problem of printing money orders remotely by printed data on preprinted money order forms. Thus, the system of Foreman et al. requires specialized printing stations.

Further, in US Patent No. 5,909,673 issued to Gregory, incorporated herein by reference, a system uses remote printing stations to print coupons on blank paper. However, such a system does not prevent a malicious party to intercept the data fed to the printer and make multiple copies. It also does not prevent copying of the printed document. This poses a problem for documents which are negotiable.

Further, in many of the conventional systems, access to a central databas or server is needed to authenticate the printed document. This is problematic.

It is an object of the present invention to provide a technique which alleviates the above drawbacks.

SUMMARY OF THE INVENTION

According to the present invention we provide a method of remotely processing a document securely, comprising: providing a communication link between a certified document owner and a remote printing station; providing said printing station with a leaf of recording media; determining by said printing station, whether said leaf is legitimate; transmitting, using a first key, from said printing station to the certified document owner a representative number of said leaf; appending, by said certified document owner, said document with said representative number; computing, by said certified document owner, a digitally signed version of said appended document, by a second key; and sending by the certified document owner, the document and said signed version, to said printing station.

In a first aspect of the present invention, a method and system for remotely processing a document securely, is provided which includes providing a communication link between a certified document owner and a remote printing station, providing a leaf of a recording media (such as special paper, cardboard, etc.) to the remote printing station, determining by the printing station, whether the leaf is legitimate, and transmitting, by the printing station, information comprising a representative number $N(L)$ of the leaf, appending, by the certified document owner, the document D with $N(L)$, encrypting or digitally signing, by the certified document owner, said appended document to generate code $Pr2(D,N(L))$, and sending by the certified document owner, the document D and the encrypted (or signed) version $Pr2(D,N(L))$ of the appended document to the printing station to be both printed by the printing station.

With the invention, negotiable documents can be securely and reliably printed remotely by third party printing stations. Further, non-authentic additional prints and copies of the same document can be easily recognized by publicly available means.

The present invention also has the advantage of preventing an adversary or unscrupulous person from making an undetectable alteration in

the content of an otherwise authentic document (e.g., such as using typewriter correction fluid to change a failing grade to a passing one on a transcript). Such changes to the document content would cause it to no longer match the signature *Pr2(D,N(L))*.

Further, unlike the conventional systems, in which access to a central database or server is needed to authenticate the printed document, in a preferred embodiment of the present invention, the printed document can be authenticated using publicly available means without needing to contact the owner and/or the issuer of the document.

For greater security, such publicly available authentication capabilities can be combined with authentication mechanisms which are secret. Then, the party that wants to produce counterfeited documents is left with a doubt about whether the secret mechanism has been broken or not. In particular, one can easily use several embodiments of the present invention in the preparation of a single document, where some embodiments allow for public authentication and others do not.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of preferred embodiments of the invention with reference to the drawings, in which:

Figure 1A is a block diagram of an exemplary format for a document printed according to the present invention in one preferred embodiment;

Figure 1B is a block diagram of a system according to the present invention;

Figure 2A is a flow diagram representing how the information needed to produce a document is processed;

Figure 2B illustrates authentication of a document being performed by a central server 230 by a remote printing station P1 sending information on the document securely to the central server;

Figure 2C illustrates a smart card (or radio frequency identification tag) affixed to a leaf of media *L*;

Figure 3 illustrates an exemplary information handling/computer system for use with the present invention; and

Figure 4 illustrates a storage medium 400 for storing steps of the program for producing a document by a remote printing station *Pi*.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Referring now to the drawings, and more particularly to Figures 1-4, preferred embodiments of the present invention will be described.

Before proceeding to the description of the present invention enabling such remote printing, the domain of application of the present invention will be addressed.

A document to be printed can be attached to a single, easily identifiable entity (e.g., person, institution, etc.) or not.

The second case (when no designee is mentioned on the document) is more delicate and is the subject matter addressed by the present invention. The second case applies for instance to negotiable documents.

To describe the present invention, some concepts and tools from modern cryptography will be described.

More precisely, secret key cryptography, as well as *private key/public key pairs* (in the form of *public encryption schemes* or of *public digital signature schemes*) and *secure hash functions* (e.g., such as the Secure Hash Algorithm (SHA-1)) will be used in the present invention. The use of secret key cryptography, of private key/public key pairs, and of secure hash functions are now well-known. For example, a description of these techniques and various implementations can be found in "Handbook of Applied Cryptography", by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press, 1997 and in "Cryptography, Theory and Practice" by Douglas R. Stinson, CRC Press, 1995.

For definiteness, each time a private encryption scheme is used, one can choose the Rivest-Shamir-Adleman (RSA) protocol, described in US Patent No. 4,405,829, incorporated herein by reference, as a method to generate and use a private/public key pair in order to allow for public encryption. Several other methods could also be used such as elliptic

curves (see, *e.g.*, the "Handbook of Applied Cryptography" and "Cryptography, Theory and Practice", both cited above).

In the description below of the present invention, it is described that a document or an image is encrypted using, for example, some private key. It is indeed assumed that the document or image is interpreted as a number to which cryptographic methods can readily be applied. If the corresponding number is too long, a hash function can be used to reduce the information, and/or one can cut the number into smaller components. The hash function which is used will be made publicly known if public key cryptography is to be used. These are all practices well known in the art, which need no further description below.

As described below, the present invention discloses how a certain Certified Document Owner (or hereafter a "CDO") C can remotely print a document D at one of a plurality of remote Printing Stations P1, P2,..., so that neither the station Pi (e.g., where i = 1, 2, ...) where the document is printed, nor any other party possessing a printer can, at reasonable cost, print a copy of D which can be mistaken for an authentic document.

Further, it is ensured that a photocopy of the document cannot be mistaken for an authentic document.

Moreover, it is ensured that a great part of the authentication, if not all, can be performed by using publicly available means and possibly without the need to contact a centralized database or authority.

Additionally, in circumstances where several original copies of the document are needed (e.g., for death certificates in some countries), several copies can be remotely printed, whenever accepted by the CDO.

It is noted that the CDO does not need to communicate directly with the printing stations. As documents can be circulated securely between computers in electronic form, using well-established cryptographic means, the CDO can delegate the contact with printing stations to a dedicated agency or a plurality thereof. Such agencies can also function as entities for authenticating documents. The simultaneous use of several agencies allow to use the Information Dispersal Algorithm (IDA) (as described for instance in the "Handbook of Applied Cryptography") so that collusion between several agencies is needed to forge documents. Such a del gation would not modify the basic mechanisms in the present invention and thus

will not be described further herein. However, it is noted that the present invention, together with a dedicated portal such as Vouchsafe, represents a new type of business, including the sale of the special paper described in the present invention.

Referring now to Figure 1A, the present invention will be described. A document D, represented as a digital file is to be printed remotely. The present invention allows a printed document *Dpr(N(L))* (shown in Figure 1A) corresponding to *D* to be printed at a remote printing station. The document *D* is printed as *Dpr(N(L))*, according to instructions transmitted by the certified document owner (CDO) C to a printing station (e.g., remote printing station) *Pi* over a network such as an intranet, the Internet or the like, on a leaf *L* of special paper 100 carrying a number *N(L)* 101 of the leaf and its coded version (or its digital signature) *Pr1(N(L))*, optionally at multiple locations on *L* (e.g., 101a, 101b, 101c, etc.).

A significant portion 102 of the document D, by which is meant document D before the addition of any extra data provided for security reasons, may comprise an image(s) 102a and/or a text portion 102b, as shown on the leaf 100.

Part of the document *D* could be encrypted by the CDO using public key cryptography so that only the intended recipient of the document can decrypt *D* to access the relevant information, even though many parties can authenticate the printed document *Dpr(N(L))*.

A number *Pr2(D, N(L))* 103, is composed by the CDO as a function of document D, and the number *N(L)* is attached to leaf L 100, using a private key *Pr2*. The private key *Pr2* is the CDO's private key and the function can be an encryption algorithm or a digital signature algorithm.

Optionally, bar-coded versions of some data such as document D and the number *Pr2(D, N(L))* can be printed as represented at 104 and 105.

Further, an optically or magnetically detectable inclusion(s) 106 may be provided according to the mechanism described below, for enhanced security or counterfeiting resistance.

Figure 1B illustrates a schematic diagram of the inventive system for remotely processing a document securely, includes a communication link 2003 between a certified document owner (CDO) 2001 and a printing station(s)

2002 which may be a remote printing station(s). The communication link 2004 preferably includ s an intranet, the Internet (World-Wide-Web), etc. to which both the CDO and the printing station 2002 are selectively connectable.

The communication link can be made secure through well known cryptographic techniques.

The remote printing station has leaves of paper L which are obtained either from the CDO or a previously agreed upon legitimate supplier of such paper.

The printing station includes a mechanism 2002B for determining whether the leaf of paper is legitimate which invokes the scanner or other optical (or magnetic, etc.) device 2002D to read the numbers *N(L)* and *Pr1(N(L))* from a current leaf of paper *L* 2002C and using authentication algorithms as described in Menezes et al. mentioned above.

Alternatively, the scanner 2002D is not needed and the numbers *N(L)* and *Pr1(N(L))* are read off by a human operator and entered via a terminal to the mechanism 2002B for verification.

Alternatively, *N(L)* and *Pr1(N(L))* are sent to the CDO or a trusted authority for authentication.

After *L* is authenticated, the number *N(L)* is transmitted from 2002A to 2001A via printer 2003. 2001A also contains a computer/processor to initiate and/or organize the various operations of the printing station P1.

A computer/processor 2001B on the CDO's side concatenates the messages *D* and *N(L)* and possibly other data, and produces a digitally signed version *Pr2(D,N(L))* by using a second private key *Pr2*, and sends the document to the printing station 2002 to be printed by printer 2003 onto the leaf of paper *L*.

Key ownership:

Two pairs of keys *(Pr1, Pu1)* and *(Pr2, Pu2)* in some standard public key cryptography systems are used. *(Pr1, Pu1)* is the pair used to sign the leaf of paper L while *(Pr2, Pu2)* is used by the CDO to sign *(D, N(L))*. Ther fore, the private key *Pr2* should belong to the CDO. The leaf L can be signed by the certified paper producer (CPP), the certified document

owner, trusted authorities or a combination thereof in which case, these parties are the owner of the pair *(Pr1, Pu1)*.

The remote station verifies this signature (either by using *Pu1* or submitting it to some trusted authority). The printing station also forwards the pair *(N(L), Pr1(N(L))* to the CDO so the CDO can also verify the legitimacy of the leaf L. In an extension of the invention, one or more CPPs provide papers to one or more remote printing stations, who in turn work with one or more CDOs.

Figure 2A represents a process 2000 of the flow of information to be exchanged between a certified document owner C 2001 and a remote printing station *Pi* 2002, in the standard case when only two pairs of keys are used.

In the process 2000, first, in step 201, the remote printing station *Pi* determines whether the leaf L 100 is legitimate. That is, the remote printing station checks that the leaf L is legitimate by reading the pair *(N(L),Pr1(NL))* and checking whether the pair is compatible, using, for example, the public key *pu1*. The public key is provided by the CDO as the public part of the private/public key pair *(Pr1, pu1)*.

Then, in step 202, *Pi* transmits the pair *(N(L), Pr1(N(L)))* to the CDO C who can also perform the authenticity check at step 203.

Then, the CDO C computes *Pr2(D, N(L))* at step 204.

In step 205, the CDO C sends document D and *Pr2(D, N(L))* to *Pi*.

Thereafter, in step 206, the remote printing station Pi can print *Dpr(N(L))* using a printer 2003 whose characteristics are not necessarily known by the CDO, but would preferably be known if images are to be printed as explained above.

In the present invention, it is assumed that the CDO C and each of the printing stations P1, P2,... is equipped with a computer capable of handling basic functions such as, for example, the computing power needed to handle public key cryptography and other cryptographic functions.

It is also assumed that C is linked to each of P1, P2, ... by electronic communications, which may or may not be secure (e.g., the electronic communication needs not be secure). Hereinbelow is first described the fundamentals of the invention, which provides a level of

security quite adequate for s veral applications. Then, it will be described how the invention can be further enhanced and complemented to ensure higher levels of security. Th highest levels of security require some private cryptography or backup by electronic documents, while very high levels of security are already accessible using only public cryptography and paper documents handling.

Copy, Counterfeit and Tamper Prevention

First, it is assumed that photocopy-protected paper as described above is used. Such paper is presently used, for example, for college transcripts and some checks and negotiable instruments. The transcript and the check cases are simple as the issuing institutions have full control of the production of the documents, a simplification incompatible with delocalized printing.

To mitigate this loss of full control, each leaf of legal paper *L* will carry (e.g. printed on *L*) a number *N(L)* and a coded (or digitally signed) version *Pr1(N(L))* of *N(L)*, where (*Pr1*, *pu1*) is the first (Private key - public key) pair, controlled by the CDO C or some other party as explained above in the section "Key Ownership".

Preferably, a requirement on *L* is that *N(L)* and *Pr1(N(L))* are hard to remove, modify and tamper with and still look authentic. For example, *N(L)* and *Pr1(N(L))* can be printed with special inks and or processes such as those provided by Verify First Technologies. *L* can also carry a mark indicating its monetary value, either coded or non-coded, in case the fee for making the document is included in the value of leaf *L* when leaf *L* is purchased. Any of the printer owners can check whether a leaf of paper *L* is authentic by using the public part (e.g., *pu1*) of the key pair. The special paper can have several document- types uses or a single document-type use.

For further protection, the CDO can keep track of which numbers come in possession of any given printer station *Pi* by a database 2001C shown in Figure 1B.

Further Print Prevention (no image protection yet)

When printing document *D* on a leaf of paper *L*, leaf *L* is read by a optical/magnetic scanner 2002D, shown in Figure 1B, to obtain *N(L)* and *Pr1(N(L))*, residing at the location of printer *Pi*, which sends

electronically the pair *(N(L), Pr1(N(L)))* to the CDO C and/or any other authenticating entity.

For some uses (e.g., for movie tickets), a human operator could also read *N(L)* and *Pr1(N(L))* directly from *L* and these data would be keyed in to be sent to CDO C and/or any other authenticating entity. Optionally, the printing station *Pi* can also send *Pr1(N(L))* to CDO C for authentication of the paper *L* by CDO C.

Then, CDO *C* sends document *D* and *Pr2(D, N(L))* electronically to the printer of *Pi*, where *(Pr2, pu2)* is the second (Private key - public key) pair, and *Pr2(D, N(L))* denotes the result of encrypting and/or signing the concatenation of *D* with *N(L)* by the private key *Pr2*. For this purpose, key management, such as obtaining proper digital certificates, are handled by 2001D. Both document *D* and *Pr2(D, N(L))* are printed on leaf *L* resulting in the printed document *Dpr(N(L))*. Anyone in possession of the printed version *Dpr(N(L))* of the document *D* can check for its authenticity by using *pu1* and *pu2*. The authentication of *Dpr(N(L))* can also be performed by a central server or trusted authority by sending the information on the document (such as a scan of the document) to the central server or trusted authority.

For example, as shown in Figure 2B, a remote printing station P1 sends *N(L)* and *Pr1(N(L))* to a central server 230. The central server 230 determines whether *Pr1(N)(L))* is a digital signature of *N(L)* and informs the printing station P1 whether leaf *L* is authentic or not.

Pr2(D, N(L)) and possibly *N(L)* and *Pr1(N(L))* can be printed on *L* in a variety of formats (e.g. text, 1-D or 2-D bar-codes, etc.). The reading of *Pr2(D, N(L))* then occurs using the appropriate technologies, i.e. optical character recognition (OCR) when text is printed (in which case a OCR-friendly font is preferable), bar-code reader when bar-codes are used. Magnetic inks such as MICR toner can be used to facilitating reading using a magnetic scanner. Of course, several of these printing formats can be used in conjunction by anyone skilled in the art.

Alternatively, or in complement, *Pr2(D, N(L))* may be printed on the leaf *L* as a modulation of the background in light color patches where, for instance, the light r or white patches would corr spond to "0"s, and th darker small patches would correspond to "1"s.

Another key can be chosen for the background, such as, for example, secret key cryptography (or a combination of public keys and secret keys in various parts of the document). In such a case, the background could be chosen as an implementation of the watermarking technique described in US Patent No. 5,825,892 to Braudaway et al, incorporated herein by reference. To control such a watermark, proper alignment, as described for instance in U.S. Patent Application No. 09/240,212, filed on 1/29/99 by Gordon Wesley Braudaway and incorporated herein by reference, may be employed. Such watermarks are detectable even if the document is printed by a reasonably-priced printer such as an Epson Stylus 700 or the like.

In yet another preferred embodiment, a method and system is provided which also uses copy resistant media, each unit (leaf) L of which contains a unique identifying character string $N(L)$ and a digital signature $Pr1(N(L))$ of the character string. This embodiment will not use public key cryptography, but only secret key cryptography. This corresponds to a different business model where, instead of providing a solution with maximal ease of use to the end customer, one requires authentication to appeal to some agency which then charges for this service and engages its responsibility as guarantor of the authenticity.

As mentioned previously, it may be advantageous to combine such secret key based methods with ones using public key cryptography, for instance to combine the advantage of easy checking and leave the insecure feeling to the counterfeiter that possibly, he/she could not break the secret key.

The specific textual information D to be printed on the document, is concatenated to the unique identifying character string $N(L)$ of the leaf of copy resistant media L to form a unique composite character string $Ccs(D,N(L))$ for the document. The unique composite character string is encrypted using a first secret key cryptographic method to form a first secure character string $SCS1(D,N(L))$. The first secure character string is then digitally signed, resulting in a digital signature $Ds(SCS1(D,N(L)))$.

Then some number, n, of characters from the first secure character string is selected and those n characters (e.g., the last n ones) are concatenated with the digital signature $Ds(SCS1(D,N(L)))$ and converted into a visibly identifiable binary sequence $IBS(D,N(L),n)$, (e.g., a two-dimensional bar code) that is also to be printed on the document, to

serve as a first check of the integrity of *D* and the relation of *D* with *N(L)*, thus protecting from illegal further prints.

Next, a digital image *UDI* is composed by overlaying onto a colored background, having at least one color, the nonspecific graphic and textual overlay of the document, the specific textual information of the document, the unique character string *N(L)* of the specific leaf of copy resistant media *L* (which is already printed or embedded into *L* in some form), and the visibly identifiable binary sequence.

In the next step, the first secure character string is encrypted a second time, using the second secret encryption key, to form a second secure character string *SCS2(D,N(L))*. Then *m* characters (e.g., the last *m* ones) are selected from the second secure character string as a unique key for generating a secure image Watermarking Plane *WP*.

The digital image *UDI* is then nearly-invisibly watermarked using the Watermarking Plane *WP* to form a watermarked digital image *PDI*. The image watermarking method recommended is described in U.S. Patent No. 5,825,892, incorporated herein by reference. The watermarked image is then transmitted electronically to a remote printer to be printed on the unique leaf of copy resistant media *L*.

If the document produced at the remote printer is re-digitized by scanning, and a duplicate Watermarking Plane is reproduced as described earlier, and if the specific watermark can be unequivocally extracted from the re-digitized image, positive evidence of an authentic document is obtained. If further inspection of the copy resistant media shows no evidence of copying, tampering or alteration, further evidence of authenticity is obtained.

If the specific textual information and the unique media identifying character string are electronically read from the printed document (e.g., using an optical character recognition (OCR) method), and they, when digitally signed and encrypted with the first secret cryptographic key, produce the same visible binary pattern *IBS(D,N(L),n)* as also read from the printed document, still further evidence of document authenticity is obtained. If all of the evidence so obtained is affirmative, the printed image that was r -digitized is deemed to be authentic.

In some cases, the document to be printed contains private information that is not to be indiscriminately divulged, such as, for example, a medical record. In that case, the composed protected document, as a whole, is further encrypted using public key encryption so that only an authorized recipient knowing the appropriate private key can decrypt the document and produce a human-readable image for printing.

In some cases, *D* can contain some extra data such as a date, location, etc. Also one may choose to include *N(L)* in document *D* so that a quick inspection would reveal whether there is a match between what is printed by *Pi* and the number *N(L)* as written/deposited on the paper before it is delivered to printing station *Pi*.

In case several authentic copies are needed, the CDO will send printing instructions corresponding to all leaves of legal papers to be used, and will preferably keep track of how many legal prints are made. Note that *Pr2(D, N(L))* and the printed document *Dpr(N(L))* depends on the *N(L)* and thus each authentic copy is different.

Image Protection in the Above Scenario

Images can be considered as parts of the document for all encryption purposes. To that effect, the CDO should publicly disclose how the different parts of the document (e.g., text portions and images), are handled in digital form to form the message to be treated by the chosen encryption scheme. One source of difficulty here is the fact that images must be printed on the document and subsequently scanned for authentication. The process of printing and scanning, especially when the specific printers and scanners used are not known, generates errors in the image which must be dealt with.

Alternatively, when the image is simple enough, a textual description of the original image can be printed on the document (in addition to the image), and part of the verification of the document would include checking that the scan of the printed image is an acceptable modification of the printed description of the image.

In the present invention, preferably the key pairs are changed as time passes, and dates are included in documents for improved protection.

Additionally, assuming that the special paper is hard to counterfeit, eavesdroppers cannot use signals transmitted between the CDO C and the printing station *Pi* to create authentic copies of the document.

However, an eavesdropper might be able to use the content D and other transmitted data between C and *Pi*, which are confidential in some cases, for other malicious purposes. In this case, a secure communication channel can be established between *Pi* and C using well-known cryptographic techniques.

For example, one way to do this is to use the remote printer *Pi's* public key *pu3* for all communication from the CDO to the printing station *Pi*, where *(Pr3, pu3)* is the third (Private key - public key) pair, and the CDO public key *pu4i* reserved to *Pi* for all communication from *Pi* to the CDO, where *(Pr4i, pu4i)* is the *i-th* element of a fourth collection of (Private key - public key) pairs. It is noted that *(Pr3, pu3)* and each *(Pr4i, pu4i)* are public encryption schemes, while *(Pr1, pu1)* and *(Pr2, pu2)* are public signature schemes.

Another desirable property of the communication channel is fault-tolerance. For example, if the communication is interrupted during the remote document printing protocol, both sides share the same belief as to whether the document has or has not been printed. Several protocols can be put in place to handle transmission breaks and/or paper jams, depending on the level of security required. One very secure method includes first sending all printing instruction(s), and, after the printer station acknowledges proper printing of the document by some communication means such as the Internet, the telephone or the like, a further digital signature is transmitted which can then be printed or written by any other means on the document.

For even higher protection, variations of the above techniques and practices may be selectively employed.

For example, instead of the kind of special paper described above, which has been so far only characterized as offering protection against photocopying and digital scanning, and carrying distinct pairs *(N(L), Pr1(N(L)))* on each leaf L, sp cial paper could be used with hard-to-imitate texture and/or marks and/or inclusions (e.g., one still may choose that such special paper carry the photocopy protection discuss d above, and such

a solution is preferable, although photocopy protection is ensured using the random inclusions in the way described below).

For example, a very high degree of security can be achieved when using Special Paper with Random Marking (SPRM), where the randomness is such that two identical or very similar specimens are difficult (if not impossible) to produce. Such papers have the property that they are difficult to counterfeit.

Examples are given by magnetic or visible inclusions (e.g., such as inhomogeneities in the paper, fibers with different optical properties than the rest of the matter of the paper, etc.) mentioned above with regard to the document shown in Figure 1A. The sizes, shapes, positions, and more generally any characteristics of the inclusions, or a collection of the bigger inclusions (e.g., in fixed number, or above a given size) can be used to determine the number $N(L)$ using again public key encryption, or are recorded as an extra number $N'(L)$ which will be used by the CDO in the composition of what needs to be printed at Pi.

Including the random markings in the composition of $N(L)$, which is then signed as $Pr1(N(L))$, by the paper producer also enhances preventing counterfeiting by a malicious document printer. Otherwise, the CDO has no assurance that the data allegedly derived from the SPRM was actually derived from SPRM, rather than from some forged paper that the malicious printer can easily duplicate. More precisely, while the use of $Pr1$ prevents attacks where the malicious party would create false leafs at will, this malicious party can read legitimate leafs and produce false clones when $N(L)$ is not linked to an unreproducible feature of the leaf L.

For example, if $M(L)$ is the number obtained by concatenating, in some prescribed way, the numerical characteristics of the ten bigger inclusions (e.g., the row and column numbers of the element of the grid Gr, as described below, which are partly covered by the big inclusions, the resonance frequencies of some electromagnetic inclusions, etc.) $N(L)$ or $N'(L)$ can be chosen as $M(L)$ or as the hashed and/or encrypted version of $M(L)$.

For a magnetic inclusion, a separate reader would be needed to authenticate a leaf L, and later the document printed on L, while in the case of a visible inclusion, such as random density variations in the paper texture, a optical scanner as described above may suffice.

The location of the inclusions will be made according to some grid Gr whose coarseness may depend on the application (e.g., finer grids generally require more expensive equipment for more precise reading). Leafs which contain inclusions which are to be considered in the computation of $N(L)$ or $N'(L)$ and which are at locations which are ambiguous, will be discarded. $N(L)$ and/or $N'(L)$ are computed by the paper manufacturer who may use a high quality scanner or other instrument depending on the nature of the inclusions. That is, leafs which may produce non-predictable results about which are the bigger inclusions when read by a lower quality scanner will be discarded.

In all cases, it is important that the texture of the paper allows for visual inspection to determine whether the paper has not been tampered with and/or to modify the locations of the inclusions. This tampering is quite hard if many inclusions participate in the computation of $N(L)$ or $N'(L)$. One can also use the smaller inclusions as a qualitative check of the authenticity of the paper.

A simpler, but possibly more costly solution for increased security is to adjoin a smart card 250 with unique marking, or a radio frequency identification (RFID) tag 250' with a one of a kind signature, to the document, as shown in Figure 2C. Then, as in the case of SPRM, $N(L)$ will be chosen as a possibly coded version of the one-of-a-kind signature $M(L)$ of the leaf of SPRM, or of the smart card 250, or of the RFID tag 250', or of a similar device.

In these cases, $N(L)$ is not necessary a number printed on L, but is determined and/or computed by reading the characteristics of L while $Pr1(N(L))$ is printed on L for verification.

For even further levels of security, as is done for very sensitive documents such as currencies, it is always advisable to complement the publicly-available verification mechanism by secret protections known only by a few affiliates and or employees of the CDO. Indeed, one may choose that no one knows the full collection of authentication marks.

In the case of documents such as death certificates, where usually a fe is paid to the corresponding agency for creating such documents, the fee can be collected either electronically every time the data is sent to Pi for printing, or the fee is paid at the time the paper is purchased, in which case a mark denoting the fee paid could appear in the paper.

In the case the system is devised for very general use, preferably the special paper is devised to have a rather low cost.

Fully verifying the authenticity of a document comprises reliably reading *N(L)*, *N'(L)* and verifying all the appropriate signatures. Since such actions may not be easy for an ordinary user of paper documents, a verification agency could provide these services preferably for a fee. (Each such agency could easily work with documents from multiple CDOs, CPPs and printing stations.)

While the overall methodology of the invention is described above, the invention can be embodied in any number of different types of systems and executed in any number of different ways, as would be known by one ordinarily skilled in the art taking the present specification as a whole.

For example, as illustrated in Figure 3 , a typical hardware configuration of an information handling/computer system for any of the printing station *Pi* and/or the certified document owner's side (please confirm that this drawing is acceptable and , in accordance with the invention preferably has at least one processor or central processing unit (CPU) 311. The CPUs 311 are interconnected via a system bus 312 to a random access memory (RAM) 314, read-only memory (ROM) 316, input/output (I/O) adapter 318 (for connecting peripheral devices such as disk units 321 and tape drives 340 to the bus 312), user interface adapter 322 (for connecting a keyboard 324, an input device such as a mouse, trackball, joystick, touch screen, scanner, etc. 326, speaker 328, microphone 332, and/or other user interface device to the bus 312), communication adapter 334 (for connecting the information handling system to a data processing network such as an intranet, the Internet (World-Wide-Web) etc.), and display adapter 336 (for connecting the bus 312 to a display device 338). The display device could be a cathode ray tube (CRT), liquid crystal display (LCD), etc., as well as an output device (e.g., such as a hard-copy printer 2003).

Further, while the present invention has been described primarily in terms of software or software/hardware configuration, the same or similar functions could be implemented in a dedicated hardware arrangement.

In addition to the hardware/software environment described above, a different aspect of the invention includes a computer-implemented method

for producing a document. As an example, this method may be implemented in the particular environment discussed above.

Such a method may be implemented, for example, by operating a computer, as embodied by a digital data processing apparatus, to execute a sequence of machine-readable instructions. These instructions may reside in various types of signal-bearing media.

Thus, as shown in Figure 4, in addition to the hardware and process environment described above, a different aspect of the invention includes a computer-implemented method for producing a document, as described above. As an example, this method may be implemented in the particular hardware environment discussed above.

Such a method may be implemented, for example, by operating the CPU 311 (Figure 3), to execute a sequence of machine-readable instructions. These instructions may reside in various types of signal-bearing media.

Thus, this aspect of the present invention is directed to a programmed product, comprising signal-bearing media tangibly embodying a program of machine-readable instructions executable by a digital data processor incorporating the CPU 311 and hardware above, to perform a method of processing (e.g., printing) remotely a document securely.

This signal-bearing media may include, for example, a RAM (not shown in Figure 4) contained within the CPU 311 or auxiliary thereto as in RAM 314, as represented by a fast-access storage for example. Alternatively, the instructions may be contained in another signal-bearing media, such as a magnetic data storage diskette 400 (e.g., as shown in Figure 4), directly or indirectly accessible by the CPU 311.

Whether contained in the diskette 400, the computer/CPU 311, or elsewhere, the instructions may be stored on a variety of machine-readable data storage media, such as DASD storage (e.g., a conventional "hard drive" or a RAID array), magnetic tape, electronic read-only memory (e.g., ROM, EPROM, or EEPROM), an optical storage device (e.g. CD-ROM, WORM, DVD, digital optical tape, etc.), paper "punch" cards, or other suitable signal-bearing media including transmission media such as digital and analog and communication links and wireless. In an illustrative embodiment of the invention, the machine-readable instructions may comprise software object code, compiled from a language such as "C", etc.

The present invention can of course also be used in settings where the printer stations *Pi* are specialized, tamper-resistant printing stations with special printers which would further decrease the possibility of counterfeiting. More particularly, the present inventions could have several applications in the banking industry (e.g., for more secure checks or other financial instruments).

For the case where SPRM is not used, there is a possibility that a malicious printing station can find some paper that looks like real paper to a human, but is easily to duplicate. Then, the unscrupulous person may copy *N(L)* and *Pr1(N(L))* from any legitimate document onto that paper, get the CDO to print a document on it, and be able to produce duplicate copies. In another extension of the invention, the signature *Pr1(N(L))* that proves a leaf to be authentic could be situated such that the process of printing the document destroys this signature.

For example, *Pr1(N(L))* could be printed on a tag which the printer tears off after printing the document or the heat from the printing process could evaporate the ink which prints *Pr1(N(L))*. This extension would prevent unauthorized parties from learning sufficient information to forge leafs of paper (should no SPRM or similar techniques be used); and could simplify how a CDO authenticates the printing station: if physical controls ensure that only bona fide printing stations receive authentic leafs, then a printing station can authenticate itself to a CDO by demonstrating knowledge of a *N(L)*, *Pr1(N(L))* pair.

Document Amendment

Some types of documents (e.g., car inspection stickers, transcript additions, passports, automobile titles, etc.) require a party possibly other than the original producer of the document to add an amendment under the appropriate conditions. The present invention also applies to securing the process of adding amendments to preexisting documents.

In this case, one or more Certified Amendment Owners (CAOs) would have their own key pairs *PuA-PrA*. An amendment printing station would forward *D*, *N(L)*, *Pr2(D,N(L))* to the CAO, who preferably would authenticate the document and in turn would apply the amendment *A* (which can include the date and time of the amendment plus other relevant information) and return *A*, *D*, *N(L)*, *Pr4(A,D,N(L))*, which the printer would then apply to the document, preferably along with *Pr2(D,N(L))*.

In yet another extension of the present invention, the document and signature sent to the CAO could itself contain the content and signature of a previously amended document. In this way, more than one amendment can be applied to a document.

With the invention, negotiable documents can be securely and reliably printed remotely by third party printing stations. Further, non-authentic additional prints and copies of the same document can be easily recognized by publicly available means.

CLAIMS

1. A method of remotely processing a document securely, comprising:

providing a communication link between a certified document owner and a remote printing station;

providing said printing station with a leaf of recording media;

determining by said printing station, whether said leaf is legitimate;

transmitting, using a first key, from said printing station to the certified document owner a representative number of said leaf;

appending, by said certified document owner, said document with said representative number;

computing, by said certified document owner, a digitally signed version of said appended document, by a second key; and

sending by the certified document owner, the document and said signed version, to said printing station.

2. The method according to claim 1, wherein said checking whether said leaf of recording media is legitimate comprises:

reading a pair of numbers comprising a representative number of said leaf and a digital signed version of said number from said leaf; and

authenticating said pair of numbers.

3. The method according to claim 2, wherein said authenticating said pair of numbers comprises:

transmitting said pair of numbers to said certified document owner; and

authenticating, by said certified document owner, said pair of numbers by a digital signature verification algorithm.

4. The method according to claim 2, further comprising:

transmitting said pair of numbers to said certified document owner; and

authenticating, by said certified document owner, said pair of numbers by a digital signature verification algorithm.

5. The method according to claim 2, where said authenticating said pair of numbers comprises:

authenticating, by said printing station, said pair of numbers by a digital signature verification algorithm.

6. The method according to any preceding claim, further comprising:

printing, by said printing station, the document.

7. The method according to claim 6, wherein said printing is performed by a printer at said printing station, and

wherein characteristics of said printer are known in advance by said certified document owner.

8. The method according to claim 6, wherein said document includes at least one image, and

wherein any further, unauthorized, prints and copies of said document are recognized as non-authentic prints by using only publicly available key encryption process.

9. The method according to any preceding claim, wherein said determining by said printing station includes:

reading a pair *(N(L), Pr1(NL))* including said number and a coded version of said number; and

checking whether the pair is compatible, with information controlled by said certified document owner.

10. The method according to claim 9, wherein said checking whether the pair is compatible is performed by using a public key *pu1*,

said public key being provided by said certified document owner to said printing station as the public part of a key pair *(Pr1, pu1)*.

11. The method according to any preceding claim, further comprising:

performing, by said certified document owner, an authenticity check upon receipt of a communication by said printing station.

12. The method according to claim 6, wherein said printing comprises printing said document on a predetermined printing medium.

13. The method according to claim 12, wherein said printing medium comprises printing paper having a random inclusion of at least one of a magnetic marker and an optical marker thereon.

14. The method according to claim 12, wherein said printing comprises printing said document on a photocopy-protected medium.

15. The method according to claim 6, further comprising:

linking, via cryptography, a content of what is printed with characteristics of a leaf of paper supporting the document, such that further prints cannot be recognized as authentic.

16. The method according to any preceding claim, wherein said computing includes using public key cryptography.

17. The method according to any preceding claim, wherein said certified document owner is linkable to a plurality of printing stations via an electronic communication link.

18. The method according to claim 17, wherein said electronic communication link comprises one of an intranet, a world-wide-network, and the Internet.

19. The method according to claim 6, wherein said printing comprises printing said document on predetermined paper.

20. The method according to any preceding claim, wherein each leaf of printing media carries said number of said each leaf and a coded version of said number.

21. The method according to any preceding claim, wherein said first key comprises a public key and said second key comprises a private key.

22. The method according to claim 6, wherein both the document number and the encrypted version of the document is printed on the document.

23. The method according to claim 1, wherein determining authenticity of a printed version of the document is performed by using first and second public keys.

24. The method according to claim 1, wherein authentication of the document is performed by a central server by sending the information on the document securely to the central server.

25. The method according to claim 1, wherein, when a plurality of copies are desired of said document, the certified owner transmits printing instructions corresponding to all leaves of said recording medium to be used, and monitors how many prints are made.

26. The method according to claim 1, wherein at least one of a bar-coded version of the document, the encrypted version of the document appended with the leaf number *Pr2(D, N(L)*, the leaf number *N(L)*, and the coded version of the number *Pr1 (N(L))* are provided on the printed document.

27. The method according to claim 1, wherein said encrypted version of the document appended with the number *Pr2(D, N(L))* appears as a modulation of the background in predetermined color shapes, such that one of a lighter shape and a darker shape corresponds to a "0" and the other of said lighter shape and said darker shape correspond to a "1".

28. The method according to claim 1, wherein said printed document includes the number *N(L)* such that a match may be determined between what is printed by the printing station and the number *N(L)* as formed on said recording medium before it is delivered by said printing station.

29. The method according to claim 1, wherein said document selectively includes a text portion and an image portion,

wherein said certified document owner publicly discloses how the text portion and the image portion are handled in digital form to form the message to be treated by a chosen encryption scheme,

wherein characteristics of a printer of said printing station is known in advance by said certified document owner, such that a scan of the printed document provides a digital description of the image identical to one used in said computing of the encrypted version of the document appended with the leaf number *Pr2(D, N(L))*.

30. The method according to claim 1, wherein said document includes a text portion and an image portion, and

wherein a numeric description of the original image is printed on the document, and authentication of the document includes checking that a scan of a printed image is an acceptable modification of a printed version of a numerical message describing the image.

31. The method according to claim 1, wherein said computing includes employing cryptography employs key pairs, and wherein said key pairs are changed periodically,

wherein a date is included in said document.

32. The method according to claim 1, wherein said providing a communication link comprises:

providing a secure communication channel betwe n said printing station and said certified document owner using cryptography.

33. The method according to claim 32, wherein said cryptography includes using a public key *pu3* of said remote printing station for communication from the certified document owner to said printing station,

wherein a key pair *(Pr3, pu3)* comprises a third (Private key, public key) pair, and a public key *pu4i* of said certified document owner is reserved to the printing station for all communication from the printing station to said certified document owner, wherein *(Pr4i, pu4i)* is the *i-th* element of a fourth collection of (Private key, public key) pairs,

wherein said third key pair *(Pr3, pu3)* and each said *i-th* element *(Pr4i, pu4i)* comprise public encryption schemes, and key pairs *(Pr1, pu1)* and *(Pr2, pu2)* comprise public signature schemes.

34. The method according to claim 1, wherein each said leaf carries a distinct key pair *(N(L), Pr1(N(L)))* representing said number of said leaf and said codes version of said number.

35. The method according to claim 1, wherein each said leaf comprises Special Paper with Random Marking (SPRM).

36. The method according to claim 35, wherein said SPRM includes at least one of a magnetic inclusion and an optical inclusion,

said inclusion including at least one of inhomogeneities in the recording media, fibers with different optical properties than a remaining matter of the medium, sizes, shapes, positions, and any other characteristic of the inclusion, a collection of inclusions in a fixed number or above a given size, to determine the number *N(L)* using public key encryption, or said inclusion is recorded as an extra number *N'(L)* to be used by the certified document owner in determining what is to be printed on the document.

37. The method according to claim 36, wherein, with *M(L)* being the number obtained by concatenating, numerical characteristics of a predetermined number of larger inclusions, as represented by *N(L)* or *N'(L)*, is chosen as at least one of a hashed version and an encrypted version of *M(L)*.

38. The method according to claim 36, further comprising:

with a magnetic inclusion, providing a separate r ader for authenticating a leaf, and subsequently the document printed on said leaf.

39. The method according to claim 36, further comprising:

adjoining one of a smart card with a unique marking, and a radio frequency identification (RFID) tag with a one of a kind signature, to the document such that with use of said SPRM, *N(L)* is chosen as a one of a coded version of one of the one-of-a-kind signature *M(L)* of the leaf of said SPRM, of the smart card, and of the RFID tag.

40. The method according to claim 1, wherein first and second pairs of keys *(Pr1, Pu1)* and *(Pr2, Pu2)* are employed in a public key cryptography scheme,

wherein said first pair *(Pr1, Pu1)* is employed to sign the leaf of paper L and said second pair *(Pr2, Pu2)* is used by the CDO to sign *(D, N(L))*,

wherein a private key *Pr2* belongs to said certified document owner, and wherein said leaf is signed by a certified media producer, the certified document owner, a trusted authority or a combination thereof.

41. The method according to claim 40, wherein said remote printing station verifies a signature on said leaf by one of using *Pu1* and submitting said leaf to a trusted authority, and

wherein said remote printing station forwards the pair *(N(L), Pr1(N(L))* to said certified document owner such that said certified document owner verifies legitimacy of the leaf L.

42. The method according to claim 1, wherein each said leaf contains a unique identifying character string *N(L)* and a digital signature *Pr1(N(L))* of the character string, said leaf comprising a copy-resistant medium,

wherein secret key cryptography is employed such that specific textual information *D* to be printed on the document, is concatenated to said unique identifying character string *N(L)* of the leaf of copy resistant media *L* to form a unique composite character string *Ccs(D,N(L))* for the document.

43. The method according to claim 42, wherein said unique composite character string is encrypted using a first secret key cryptography to form a first secure character string *SCS1(D,N(L)), and*

wherein said first secure character string is digitally signed, resulting in a digital signature *Ds(SCS1(D,N(L)))*.

44. The method according to claim 43, wherein a number, *n*, of characters from the first secure character string is selected and said *n* characters

are concatenated with the digital signature *Ds(SCS1(D,N(L)))* and converted into a visibly identifiable binary sequence *IBS(D,N(L),n)* also to be printed on the document, thereby to serve as a first check of the integrity of *D* and the relation of *D* with *N(L)*.

45. The method according to claim 44, wherein a digital image *UDI* is composed by overlaying onto a colored background, having at least one color, a nonspecific graphic and textual overlay of the document, the specific textual information of the document, the unique character string *N(L)* of the specific leaf of copy resistant media *L* and the visibly identifiable binary sequence.

46. The method according to claim 45, wherein the first secure character string is encrypted a second time, using a second secret encryption key, to form a second secure character string *SCS2(D,N(L))*, and

wherein *m* characters are selected from the second secure character string as a unique key for generating a secure image watermarking.

47. The method according to claim 46, wherein said digital image *UDI* is nearly-invisibly watermarked using the watermarking to form a watermarked digital image *PDI*, and wherein the watermarked image is transmitted electronically to said remote printing station to be printed on the unique leaf of copy resistant media *L*.

48. The method according to claim 1, wherein random markings are formed in the composition of *N(L)*, which is then signed as *Pr1(N(L))*, by a producer of said leaf.

49. The method according to claim 1, wherein said digital signature *Pr1(N(L))* evidencing that said leaf is authentic is destroyed after printing said document.
destroys this signature.

50. The method according to claim 49, wherein said signature *Pr1(N(L))* is one of printed on a tag which said remote printing station tears off after printing the document, and printed with heat-evaporable ink such that heat from printing said document evaporates said ink.

51. The method according to claim 1, wherein said document includes a document in which a party other than an original producer of the document adds an amendment to said document.

52. The method according to claim 51, wherein at least one Certified Amendment Owners (CAOs) has its own key pairs *PuA-PrA*, and wherein said remote printing station includes an amendment printing station such that said amendment printing station forwards said document *D, N(L), Pr2(D,N(L))* to the CAO.

53. The method according to claim 52, wherein said CAO authenticates said document and applies an amendment *A*, and returns the amendment *A*, document *D*, the number of the leaf *N(L)*, and the number *Pr4(A,D,N(L))*, which said remote printing station applies to said document.

54. The method according to claim 53, wherein a date and time of the amendment is applied to said document, and wherein said remote printing station also applies the number *Pr2(D,N(L))* to said document.

55. The method according to claim 53, wherein the document and signature sent to the CAO contains a content and a signature of a previously amended document.

56. A system for remotely processing a document securely, comprising:

a certified document owner;

a printing station;

a communication link between said certified document owner and said printing station such that said printing station can receive a leaf of a recording media from said certified document owner;

means for determining by said printing station, whether said leaf is legitimate;

means for transmitting, by said printing station, a pair *(N(L), Pr1(N(L)))* to the certified document owner;

means for computing, by said certified document owner, *Pr2(D, N(L))*; and

means for sending, by the certified document owner, the document D and *Pr2(D, N(L))* to said printing station.

57. A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for remotely processing a document securely, comprising:

providing a communication link between a certified document owner and a remote printing station;

providing said printing station with a leaf of recording media;

determining by said printing station, whether said leaf is legitimate;

transmitting, using a first key, from said printing station to the certified document owner a representative number of said leaf;

appending, by said certified document owner, said document with said representative number;

computing, by said certified document owner, a digitally signed version of said appended document, by a second key; and

sending by the certified document owner, the document and said signed version, to said printing station.

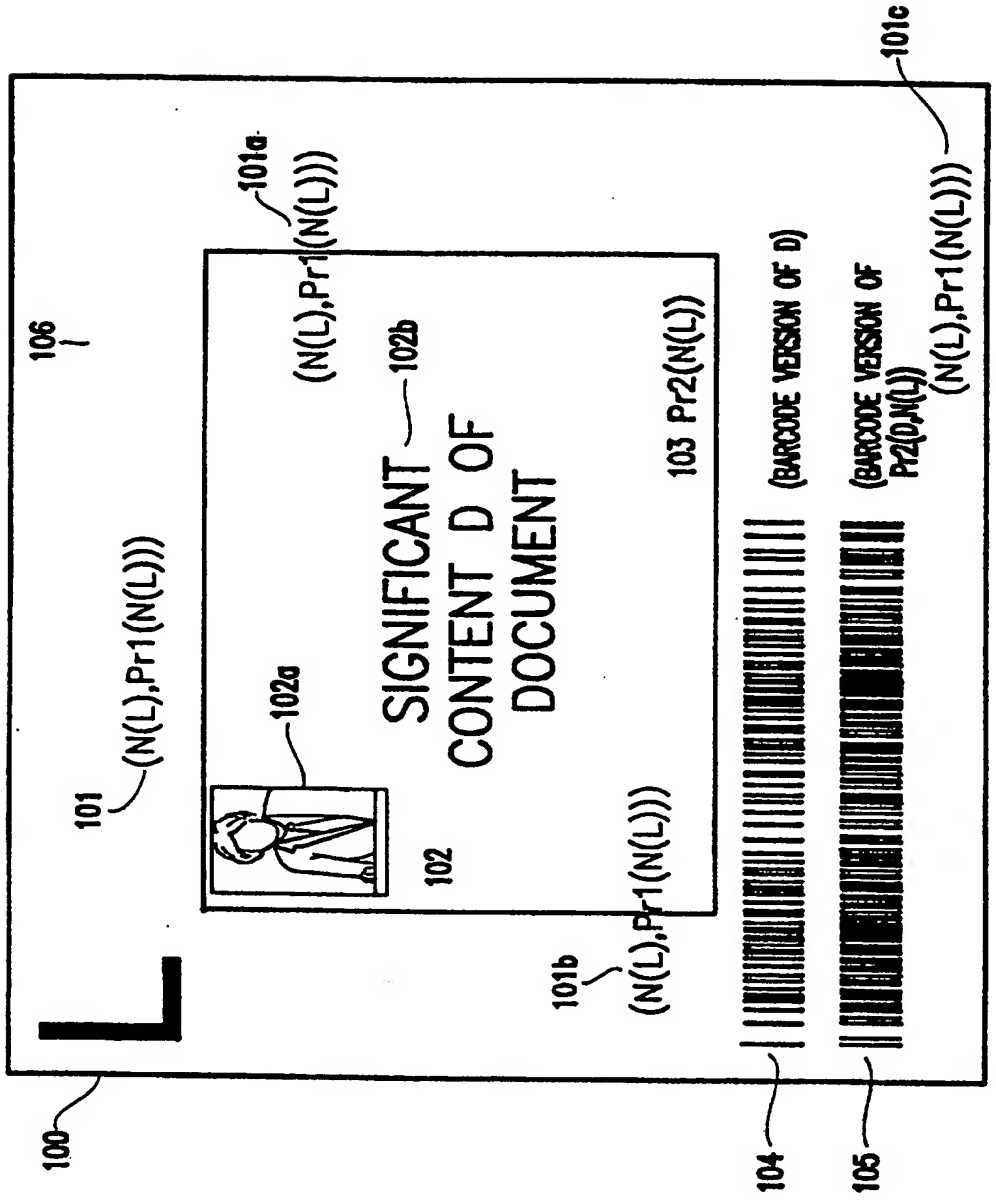
100
101
(N(L),Pr1(N(L)))
102
SIGNIFICANT CONTENT D OF DOCUMENT
102a
102b
101a
(N(L),Pr1(N(L)))
101b
(N(L),Pr1(N(L)))
103 Pr2(N(L))
104
(BARCODE VERSION OF D)
105
(BARCODE VERSION OF Pr2(D,N(L)))
101c
(N(L),Pr1(N(L)))
106

FIG.1A

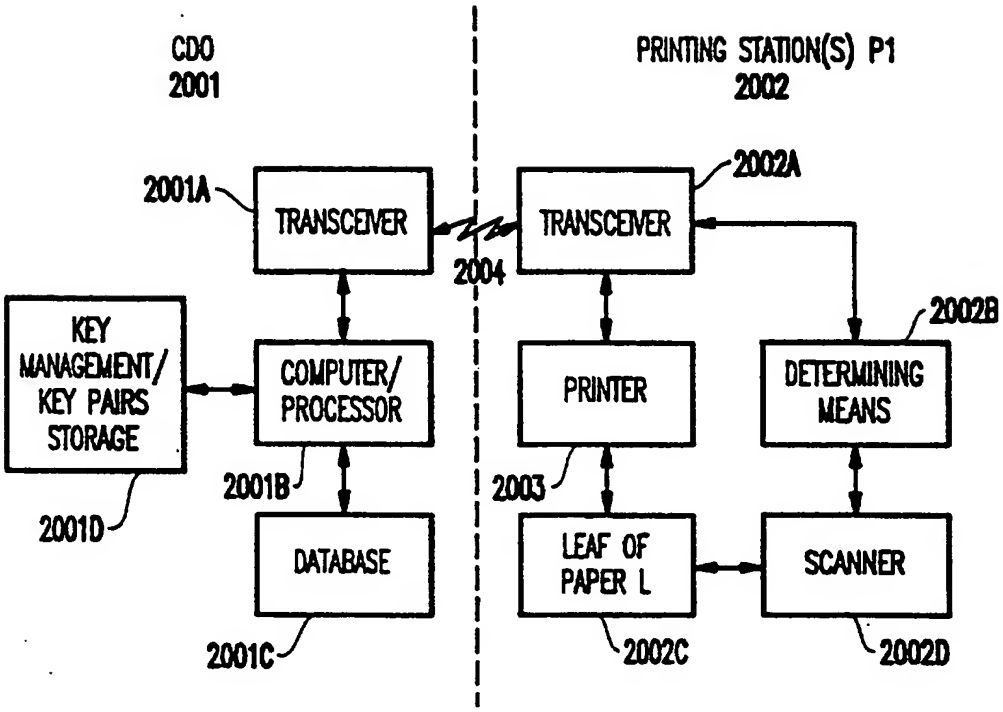
CDO
2001
PRINTING STATION(S) P1
2002
2001A
TRANSCEIVER
2004
TRANSCEIVER
2002A
KEY MANAGEMENT/ KEY PAIRS STORAGE
COMPUTER/ PROCESSOR
PRINTER
DETERMINING MEANS
2002B
2001B
2003
2001D
DATABASE
LEAF OF PAPER L
SCANNER
2001C
2002C
2002D

FIG.1B

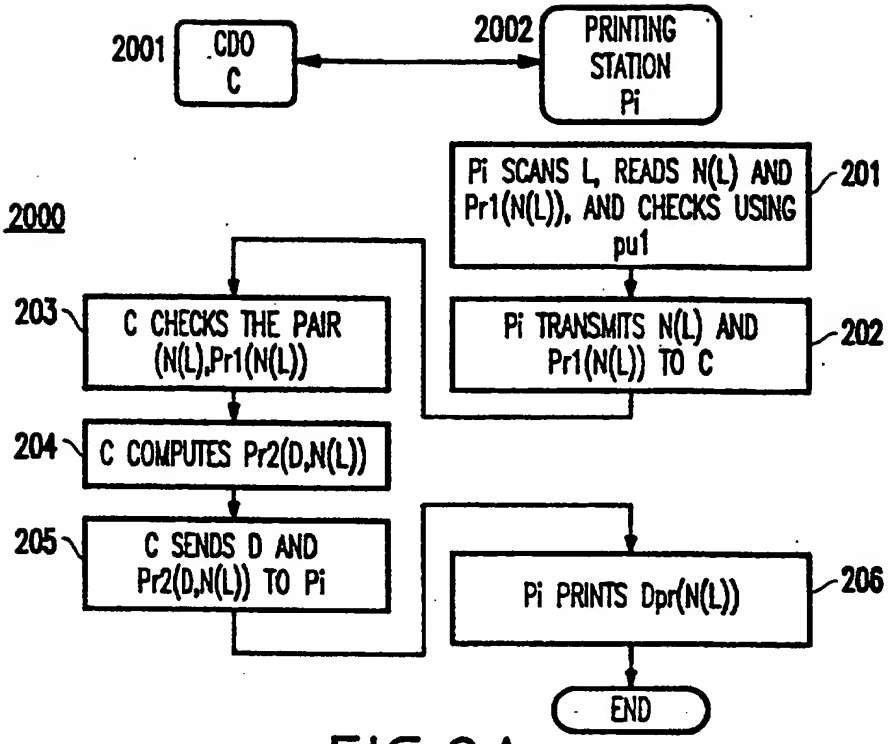

FIG.2A

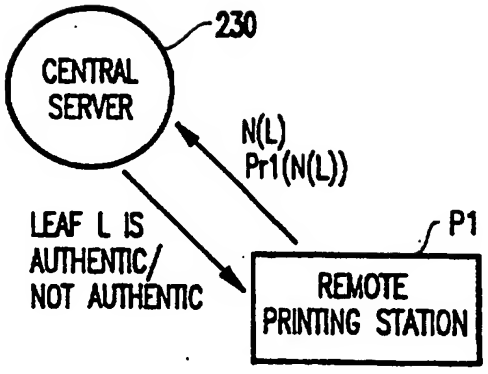

FIG.2B

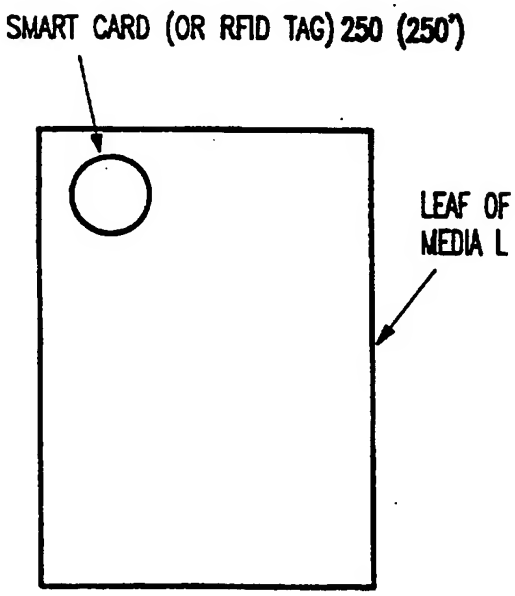

FIG.2C

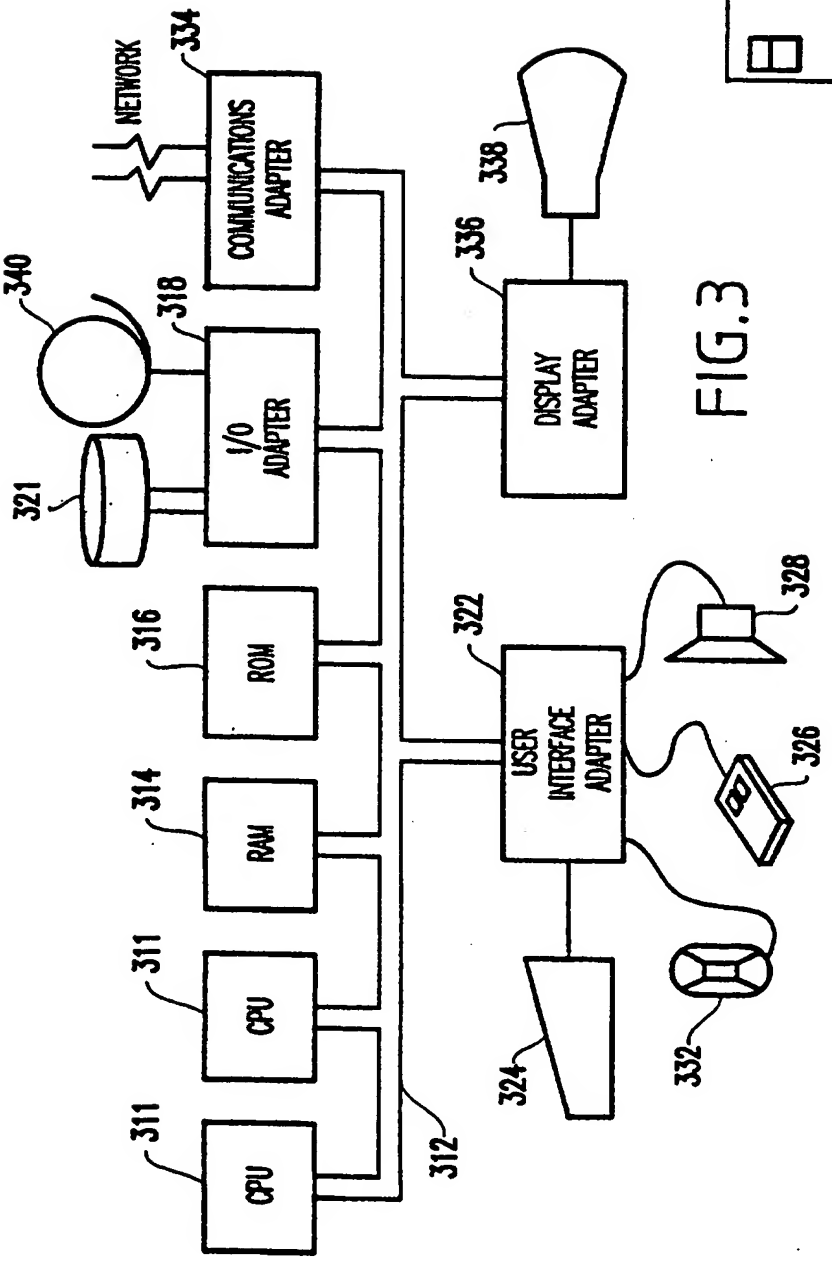
CPU
CPU
RAM
ROM
I/O ADAPTER
COMMUNICATIONS ADAPTER
NETWORK
DISPLAY ADAPTER
USER INTERFACE ADAPTER
311
311
314
316
318
321
322
324
326
328
332
334
336
338
340
312

FIG.3

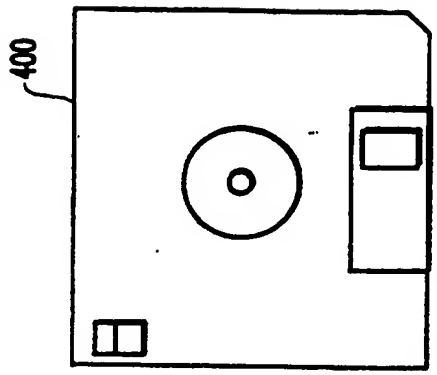
400

FIG.4

PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
The Patent Office

INVESTOR IN PEOPLE

Application No:	GB 0022614.2	**Examiner:**	Gareth Griffiths
Claims searched:	All	**Date of search:**	1 May 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4P (PDCSA, PDCSC, PDCSX)

Int Cl (Ed.7): G06F 1/00, G06K 19/06, G07D 7/00, H04L 9/00, 9/30, 9/32, H04N 1/32, 1/44

Other: Online Databases: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A,P	GB2336512 A	(INTEL)	
A	EP0935182 A1	(HEWLETT-PACKARD)	
A	WO96/25812 A1	(HUGHES)	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.